



U.S. Department of Justice

Federal Bureau of Investigation

DOCKET FILE COPY ORIGINAL
RECEIVED
FEB 17 2000
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Office of the General Counsel

Washington, D.C. 20535

February 17, 2000

Ms. Magalie Roman Salas
Secretary
Federal Communications Commission
445 12th Street, S.W.
Room TW-A325
Washington, D.C. 20554

In the Matter of:

**Communications Assistance for Law
Enforcement Act**

CC Docket No. 97-213

Dear Ms. Roman Salas:

Enclosed for filing please find an original and eleven copies of the DOJ/FBI Reply to Oppositions to Petition for Reconsideration of Section 105 Report and Order, filed by the Federal Bureau of Investigation in the matter pending before the Commission as captioned above.

Sincerely,

Larry R. Parkinson
General Counsel
935 Pennsylvania Ave., N.W., Room 7427
Washington, D.C. 20535
(202) 324-6829

cc: Public Safety and Private Telecommunications Bureau
Wireless Reference Room, Wireless Telecommunications Bureau
International Transcription Service, Inc.
International Reference Room, International Bureau

No. of Copies rec'd
List A B C D E

0211

DOCKET FILE COPY ORIGINAL
RECEIVED

FEB 17 2000

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON
OFFICE OF THE SECRETARY

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

)
)
In the Matter of:)
)

Communications Assistance for Law
Enforcement Act)
)
)
_____)

CC Docket No. 97-213

**DOJ/FBI REPLY TO OPPOSITIONS TO PETITION FOR
RECONSIDERATION OF SECTION 105 REPORT AND ORDER**

Table of Contents

Summary

Introduction	1
1. Personnel Security Obligations	2
a. List Of Limited Group Of Designated Employees	4
b. Non-Disclosure Agreements Signed By Designated Employees	8
2. Surveillance Status Message	10
3. Maximum Time To Report Suspected Compromise Of System Security	14
4. Recording Of The Date And Time Of The "Opening Of The Circuit" For Law Enforcement	16
Conclusion	18
Certificate of Service	

Summary

The Department of Justice/Federal Bureau of Investigation has asked the Commission to modify certain aspects of its regulations implementing the "systems security and integrity" mandate set forth in section 105 of CALEA. As we explained in our reconsideration Petition, although these regulations will go a long way toward ensuring the effectuation of section 105's mandate, a few key modifications are necessary to the implementation of this provision's important public purposes. In making these requests, we have focused only on those matters that federal, state, and local law enforcement officials agree are most crucial to the achievement of these important purposes. We have not merely reiterated requests previously made and rejected, but have instead carefully streamlined our personnel security requests (thereby garnering a major carrier's express support for them), asked the Commission to consider including a function that was previously requested pursuant to section 103 of CALEA, but also falls squarely within the mandate of section 105, and responded to issues that arose for the first time when the Commission released the regulations.

The commenters that oppose our requests fail to recognize the essential fact that Congress enacted section 105 to protect the privacy and security interests of the *public*, and not to maximize the convenience of telecommunications carriers. They also fail to identify any flaw in our explanations as to why the requested modifications are necessary to the effectuation of section 105. Thus, in light of their clear basis in the language and purposes of section 105, we respectfully ask the Commission to make the requested modifications to its implementing regulations.

Introduction

On March 15, 1999, the Commission released a Report and Order (SSI Order) implementing the systems security and integrity provisions contained in § 105 of the Communications Assistance for Law Enforcement Act of 1994 (CALEA).¹ On October 25, 1999, the Department of Justice/Federal Bureau of Investigation (the Department) filed a Petition for reconsideration of this Report and Order (Petition). Pursuant to the Commission's January 21, 2000 Notice (65 Fed. Reg. 3,451), several commenters filed oppositions to the Petition. The Department now replies to these oppositions.

Two general observations regarding the oppositions may be dealt with at the outset. First, they fail to recognize, or to acknowledge, that section 105 is designed to protect the privacy and security interests of the *public*. One commenter goes so far as to call the Department's position that personnel security measures are necessary to protect privacy interests "ironic[]" (BellSouth Opp. 10) — revealing the commenter's assumption that shielding the privacy interests of the general public was no part of Congress's purpose. While the Department will respond below to the objections the commenters raise in regard to particular requests, it should first be noted that the commenters' general approach to these requests suffers from an improper refusal to acknowledge section 105's essentially public purposes.

Second, several commenters claim that the Petition "simply reiterates" positions that the Commission rejected in the SSI Order. TIA Opp. 1; Motorola Opp. 1; PCIA Opp. 2; see also AT&T

¹ In the Matter of Communications Assistance for Law Enforcement Act, *Report and Order*, CC Docket No. 97-213 (rel. Mar. 15, 1999), *modified by* In the Matter of Communications Assistance for Law Enforcement Act, *Order on Reconsideration*, CC Docket No. 97-213 (rel. Aug. 2, 1999); *summary published in* 64 Fed. Reg. 51,462 - 51,470 (Sep. 23, 1999).

Opp. 1; USTA Opp. 2; Bell Atlantic Mobile Opp. 2. This claim is false. Two of the alterations to the implementing regulations sought in the Petition, relating to background checks and non-disclosure agreements, do derive from earlier requests that the SSI Order rejected — but the Petition requests only modified and limited versions of these obligations, which the Department has carefully pared down to avoid trenching upon the concerns that led the Commission to reject the prior versions. Petition at 5-6; see also SBC Opp. 2 (supporting the Petition's "modified position" regarding these obligations). The Department's requests relating to the reporting of system compromises and recordkeeping respond to the language included in the implementing regulations that the Commission released together with the SSI Order, rather than to the Commission's rejection of any requests made by the Department. Petition 9-11. (Our Petition did *not* reiterate the Department's earlier request for a two-hour maximum reporting time, and the Department had not made any request regarding the pertinent aspect of the recordkeeping requirement, because it had no objection to the version of the relevant language included in the Commission's Notice of Proposed Rulemaking. Petition 11.) The remaining request, relating to the need for an automated surveillance status message, was not previously requested pursuant to section 105, but was requested (unsuccessfully) in the section 103 proceeding. Petition 8-9. Thus, none of the requests included in the Petition constitutes a mere "reiteration."

With these general observations in mind, we turn to the commenters' objections to the specific requests set forth in the Petition.

1. Personnel Security Obligations

In the Petition, the Department explained that any protocol for ensuring that interceptions are activated "only in accordance with a court order or other lawful authorization," and only by

individuals who are "acting in accordance with regulations prescribed by the Commission" (CALEA § 105), must include some reliable mechanism for ensuring the trustworthiness of the private-company employees who have become increasingly responsible for implementing electronic surveillance. Petition 2-3. The Petition acknowledged that the SSI Order rejected the employee background check and non-disclosure agreement provisions sought by the Department to meet this concern, *id.* at 5, but noted that commenters representing a substantial portion of the telecommunications industry had either expressly supported these requests, or indicated that the obligations would require no substantial departure from their existing practices. *Id.* at 3-4 & nn.3, 4.

In order to remove the concerns that were raised by those commenters that opposed these requests, and that motivated the Commission to reject them, our reconsideration Petition substantially narrowed the scope of the requests. The modified request would apply only to those carrier employees who, as a regular part of their job duties, are exposed to information identifying the individuals whose communications are being intercepted pursuant to lawful electronic surveillance. *Id.* at 5. Carriers would be required to maintain a list of this limited group of employees, including their names, dates of birth, social security numbers, and workplace telephone numbers, which would be made available upon request to law enforcement agencies in order that they may conduct appropriate background checks on these employees. Petition 6-7. Carriers would also require these employees to sign nondisclosure agreements whereby they would agree not to make improper disclosures of sensitive information related to electronic surveillance, and to cooperate with law enforcement as necessary for the completion of appropriate background checks. Petition 7.

Acknowledging the Department's modification of these requests, one industry commenter now expressly supports them, declaring that the modification "establishes a defensible balance" between relevant competing concerns. SBC Opp. 2.

a. List Of Limited Group Of Designated Employees

Of the commenters that previously expressed their support specifically for employee background checks of designated employees, see Petition at 3 & n.3, one filed no opposition, and the other — an industry association that states that it represents tens of thousands of licensees — filed an opposition that makes no mention of this particular request (in light of which it seems reasonable to assume that this group does not object to it). See PCIA Opp.

Several commenters oppose even our significantly modified request, but their arguments are misguided. For example, some commenters assert that the very suggestion that background checks are necessary to implement section 105 "assume[s] a lack of professionalism among carrier employees." Motorola Opp. 6; see also CTIA Opp. 2; AT&T Opp. 4; NTCA Opp. 4; TIA Opp. 5-6. But personnel security measures, and the statutory mandate underlying them, assume only that the public's interest in privacy is weighty enough to require some means of ensuring the proper treatment of sensitive information. Thus, the Department's extensive checks on its own employees (see Petition 2 note 2) are based on the need to protect the privacy and security of members of the public — not on any assumed "lack of professionalism" among government employees. (Likewise, the industry commenters that expressly supported the use of background checks (*see supra*) presumably premised their support upon the practical need for security measures, rather than upon any assumption that carrier employees lack professionalism.) The government has never required the public to rely merely upon its unverified faith in the integrity of its law enforcement officials for

assurance that the confidentiality of electronic surveillance information would be respected, but has instead conducted extensive background checks on these employees. Petition 2 note 2. The public should not be compelled to rely upon private companies' unverified faith in their "trusted employees" (AT&T Opp. 4) now that the process of conducting electronic surveillance is increasingly passing into the hands of carrier employees.

The rhetorical device of placing a burden of proof upon the Department, and declaring that the Department has failed to carry it, sheds no light on the issue of whether these measures are needed. See CTIA Opp. 2; Bell Atlantic Mobile Opp. 5; BellSouth Opp. 6. The Department cannot plausibly be required to cite documented cases in which interceptions have been compromised by a carrier's employees, because it is the carriers — and not law enforcement — that control this information. A carrier might not discover such a breach at all, and if it did, the carrier's comments suggest that it would be likely to deal with the matter internally. See BellSouth Opp. 6 (urging the Commission not to give law enforcement "oversight" responsibility" for a carrier's employees); AT&T Opp. 4 ("carriers are more than competent to internally monitor security concerns"); Bell Atlantic Mobile Opp. 5 (characterizing the Department's request as an "intrusion by the government into carriers' security practices").

The commenters' assertion that even the limited background checks included in the Department's modified proposal would be impermissibly invasive (Bell Atlantic Mobile Opp. 5; Motorola Opp. 6-7; CTIA Opp. 2-3; NTCA Opp. 4) fails to recognize either the modest nature of the checks now proposed, or the privacy and security interests of the general public that the checks are designed to protect. In light of the extremely weighty nature of these public interests, it is

noteworthy that *no* commenter disputes the Department's observation that the proposed checks would be no more "frightening" (TIA Opp. 5) than those routinely conducted by landlords deciding whether to rent out apartments. Petition 6; cf. CTIA Opp. 4. These minimal investigations, which merely examine criminal and credit records pertaining to a limited group of carrier employees with regular access to particularly sensitive information, surely cannot be considered so invasive of the carrier employees' privacy as to require that serious threats to the privacy interests of the general public must be ignored.

The assertion that providing for some means of ensuring the trustworthiness of carrier employees conflicts with Congress's decision to "entrust[]" these employees with the responsibility to conduct interceptions (TIA Opp. 6; see also Motorola Opp. 6) is fundamentally misguided. Changes in the technical nature of telecommunications, rather than any legislative choice, are placing much of the process of conducting interceptions in the hands of private company employees. See Petition 2-3. And Congress's evident purpose in enacting section 105 was to check the dangers to personal privacy and security that these changes are introducing. Thus, rather than "entrusting" carrier employees with the duty of conducting interceptions, Congress directed the Commission to exercise extensive oversight over carriers, and to require them to implement systems for the effective supervision of their employees. See CALEA tit. III, § 301, *codified at* 47 U.S.C. § 229(b) (requiring the Commission to require carriers to establish policies and procedures for the "supervision and control" of their officers and employees, including policies and procedures "to prevent any * * * interception [of communications] or access [to call-identifying information] without [appropriate] authorization").

By the same token, those commenters that suggest that Congress's purpose in enacting section 105 was solely to prevent *law enforcement* from engaging in the unauthorized interception of private communications, and not to check such actions by private carrier employees, see CTIA Opp. 3; AT&T Opp. 3, overlook the plain language of the statute. Congress directed the Commission to require each carrier to "establish appropriate policies and procedures for the supervision and control of *its officers and employees*," and such policies and procedures are to be designed to "prevent *any* [interception of communications] or access [to call-identifying information] without [appropriate authorization]." 47 U.S.C. § 229(b)(1) (emphases added). The statute's plain language directs the Commission to preside over the creation of policies that will ensure that no unauthorized interceptions by *anyone* — carrier employees or law enforcement agents — may be conducted.

Two commenters insist that requiring carriers to maintain a list of employees who are designated to have regular and substantial involvement in electronic surveillance would be unduly burdensome. NTCA Opp. 4; BellSouth Opp. 8-9. But the carriers' earlier filings verify that the designation of such employees is already a common practice. See Petition at 4 n.4 (quoting from carriers' comments). Indeed, one of the very commenters that now asserts that listing designated employees would be "administratively difficult" (BellSouth Opp. 8) previously "agree[d] that it is sound practice for carriers to designate specific employees, officers or both to assist law enforcement officials in the implementation of lawful interceptions." BellSouth Dec. 12, 1997 Comments 11. As we noted in our reconsideration Petition, given the fact that carriers already generally designate employees to assist law enforcement in conducting lawful interceptions, it cannot plausibly be urged

that maintaining a list of such employees would be unduly burdensome. Petition at 4 n.5. Nor can another commenter's observations about employee turnover and the small size of some companies demonstrate any substantial "administrative[] impractical[ity]." NTCA Opp. 4. Indeed, if maintaining employee lists is as difficult for carriers as this commenter claims, it is unclear how carriers manage to determine to whom they should send paychecks every two weeks, let alone in what amounts. It is equally unclear why it would be difficult or burdensome for a rural carrier with eight employees to maintain a list of those eight employees. See *ibid.*

b. Non-Disclosure Agreements Signed By Designated Employees

To the extent that some commenters specifically object to the nondisclosure agreement request, their objections generally appear to be based upon the premise that "every new regulation that carries an obligation and a potential penalty for noncompliance is, in fact, a substantial burden." NTCA Opp. 6 (emphasis added). Apart from this policy of blanket resistance, it still remains unclear what persuasive objection may be raised against such a requirement.

One commenter insists that the requirement is "intrusive." AT&T Opp. 5. But requiring a carrier employee to acknowledge her responsibility to respect the confidentiality of information in no way "intrudes" upon the employee's privacy. This commenter also claims that the nondisclosure agreements could lead to criminal prosecutions against carrier employees, *ibid.*, but identifies no criminal provision that could be applied in reference to the violation of agreements executed between a private company and its employees. Nor is it clear, in light of the fact that (as the commenter acknowledges (*id.* at 5-6)) laws other than CALEA create duties to respect the confidentiality of information related to electronic surveillance, precisely what this commenter means by its assertion

that carrier employees should be permitted to make "independent judgment[s]," subject only to the carrier's disciplinary rules, regarding these duties. *Id.* at 5.

The suggestion that the Commission should defer to "[p]rudent business practice" and existing carrier safeguards, rather than incorporating nondisclosure agreements into the section 105 regulations, cannot be squared with the statute. BellSouth Opp. at 11-12. If Congress believed that general business practices and existing carrier policies were sufficient to protect the relevant security and privacy interests, it presumably would not have directed the Commission to oversee each carrier's mandatory development of policies designed specifically to protect these interests. 47 U.S.C. § 229(b), (c), (d). Nor does a commenter's reference to a "morass of legal consequences," which allegedly would result from the fact that nondisclosure agreements would "all but convert[] carriers into agents for law enforcement," introduce a sound objection to the request. BellSouth Opp. 12. Whatever agency relationship may exist between law enforcement and carrier employees would be the product of the changes in the telecommunications industry that have made it necessary for law enforcement agents to rely upon assistance from carrier employees to conduct electronic surveillance, and this aspect of the relationship would not be substantially affected by the execution of nondisclosure agreements.

The Department is pressing for the inclusion of these personnel security measures because the entire law enforcement community, including not only federal, but also state and local law enforcement officials, agree that they are extremely important for the effective implementation of section 105 of CALEA. We have weighed the considerations that led the Commission to reject the previous version of these requests, and have carefully modified them to remove these concerns. We respectfully ask the Commission to consider these modifications, and the significant degree to which

these measures would advance the purposes of section 105, and include these streamlined requests in its implementing regulations.

2. Surveillance Status Message

Our Petition also requested that the Commission include in its section 105 regulations a requirement that carriers provide a "surveillance status message," which would enable law enforcement agencies to confirm periodically that the software used to conduct an interception is working correctly and is accessing the equipment, facilities, or services of the correct subscriber. Petition 8-9. Many commenters object to this request, but they do so primarily on baseless procedural grounds.

Two commenters charge that our request to include the surveillance status message pursuant to section 105 is "disingenuous." SBC Opp. 1; see also BellSouth Opp. 14. This allegation is groundless. Far from trying to "conceal[]" (SBC Opp. 1) — or even to downplay — the fact that the Commission rejected the surveillance status message as a requirement of section 103, we acknowledged this fact in the first paragraph of this portion of our Petition, and noted that we do not seek to challenge that ruling. See Petition 8. We also explained that, notwithstanding the Commission's conclusion that the surveillance status message was not required pursuant to section 103, the Commission is free to, and should, conclude that this capability is required to effectuate section 105's mandate that carriers must prevent unauthorized interceptions from being effected in their switching premises. Petition 8-9.

Claims that we have failed to explain why we no longer request the surveillance status message pursuant to section 103, or that we intentionally "s[a]t on" its request that this function be required pursuant to section 105, are equally unfounded. Bell Atlantic Mobile Opp. 6; see also

AT&T Opp. 7; Motorola Opp. 2; TIA Opp. 3. As we noted in our Petition, both section 103 and section 105 include language relating to the carriers' obligation to prevent unauthorized interceptions from occurring within their switching premises. See Petition 8 (quoting CALEA § 105); *id.* at 9 (quoting CALEA § 103). We explained that we decided to request the surveillance status message pursuant to section 103 because the function appeared to fall within the same "surveillance integrity" category as the other two requests we sought under this heading in the section 103 proceeding. *Ibid.* The reason we no longer request this function pursuant to section 103 is equally straightforward: The Commission determined that it is not part of the mandate of that provision.

Several commenters assert that the Commission has already determined that CALEA does not require the surveillance status message. See SBC Opp. 3 (asserting that the Commission determined that the surveillance status message is "not within the purview of the Act"); MCI WorldCom Opp. 2 (asserting that the Commission determined that the surveillance status message is "not mandated by CALEA"); PCIA Opp. 2 (asserting that the Commission determined that the surveillance status message "is not required by [CALEA]"). This assertion is false. In fact, the Third Report and Order concludes only that the surveillance status message is not required by *section 103* of CALEA. Third Report and Order ¶¶ 101, 106, 111. The Commission has never determined that the surveillance status message is not part of the mandate of section 105 of CALEA — the subject of the instant proceeding.

Although many commenters declare that the Commission is barred from making this determination now, none explains why any law, regulation, or principle of fairness should prevent it from doing so. The Department's request for the surveillance status message on reconsideration of the SSI Order certainly does not "rel[y] on facts which have not previously been presented to the

Commission." 47 C.F.R. § 1.429(b). To the contrary, the factual issues pertaining to the surveillance status message have been extensively examined in the course of numerous rounds of comments and counter-comments presented to the Commission in the section 103 proceeding. Countless pages of discussion developed in that proceeding, minutely examining and debating the merits of the surveillance status message,² belie the remarkable assertion that "there has been no notice or opportunity to comment on this proposal." USTA Opp. 3. Moreover, even if the request could nevertheless be considered to "rel[y] on" new "facts," the governing rule would still permit the Commission to consider the request. "[C]ircumstances" plainly have "changed since the [Department's] last opportunity to present" the issue, insofar as the Third Report and Order released on August 31, 1999 determined that the surveillance status message is not part of the mandate of section 103. 47 C.F.R. § 1.429(b)(1). Furthermore, the Commission clearly could determine that consideration of the request is "required in the public interest." 47 C.F.R. § 1.429(b)(3).

The sole new issue presented here is the discrete and purely legal question of whether the surveillance status message is an appropriate part of the mandate of section 105. The commenters insist that the Commission "*must* stay the course" (MCI WorldCom Opp. 2 (emphasis added)), but offer very little explanation as to why it *should*.

Several commenters assert that section 105 is "completely unrelated" to section 103. PCIA Opp. 2; Motorola Opp. 2; AT&T Opp. 7. Assuming this is true, it is unclear why this fact should constitute a reason for the Commission to conclude that the surveillance status message does not fall

² See PCIA Opp. 4 (referring to the submission of "detailed evidence" regarding the surveillance status message by "literally hundreds" of commenters); *id.* at 5 (referring to the "extensive record" developed on the surveillance status message).

within the mandate of section 105. The conclusion that section 103, which the Commission concluded does *not* require the surveillance status message, is "completely unrelated" to section 105, could serve only to highlight the need for the Commission to take a fresh look at the request pursuant to section 105.

Some commenters urge that the surveillance status message cannot be required pursuant to section 105 because that section deals with "policies and procedures," rather than with "assistance capabilities." BellSouth Opp. 14; TIA Opp. 3; Motorola Opp. 3; NTCA Opp. 7. Again, this reasoning might have some force if the Commission had concluded that the surveillance status message *was* an "assistance capability" within the meaning of section 103. But it did not. To make their case, the commenters must demonstrate that the surveillance status message cannot properly be considered part of the mandate of section 105. Remarkably, however, although they devote quite a large proportion of their comments to opposing the surveillance status message request, the commenters fail to address the specific language of section 105 upon which the Department bases the request.

Section 105 requires each carrier to ensure "that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with * * * lawful authorization." CALEA § 105. No commenter challenges the Department's observation that the surveillance status message would directly effectuate this language, by enabling carriers and law enforcement to quickly discover and correct unauthorized interceptions occurring within a carrier's switching premises. Petition 8. There is no magic in 47 U.S.C. § 229(b)'s use of the words "policies and procedures" that counteracts the force of these observations. Indeed, the commenters' construction of the statute evidently would not prevent the

Commission from requiring carriers to draw up policies and procedures whereby the carriers' employees would manually check the status of interceptions. It is hardly plausible, then, to suggest that the inclusion of the words "policies and procedures" in 47 U.S.C. § 229 bars the Commission from requiring a measure that would have essentially the same functionality as a policy of manual checking.³

Thus, although many commenters oppose the surveillance status message request, none counters our observation that this function would directly advance the mandate of section 105 by facilitating the discovery and termination of interceptions that lack lawful authorization. The Commission should effectuate the clear mandate of section 105 by requiring carriers to provide the surveillance status message.

3. Maximum Time To Report Suspected Compromise Of System Security

We noted in our Petition that any system for the prevention of breaches in the security and integrity of surveillance will suffer lapses, and that an effective system therefore must include a mechanism for minimizing the impact of such breaches. The Commission recognized this need, but rejected the Department's specific request that carriers be required to report breaches within two hours of discovery. Instead, the Commission required carriers to report compromises "within a

³ Two commenters make technical claims related to the surveillance status message, but their arguments are misguided. Messages delivered pursuant to the J-Standard in connection with "normal inbound call activity" (SBC Opp. 3) cannot be relied upon to identify the existence of an unauthorized interception. These messages assume that the recipient knows whose facilities are being surveilled, and therefore they are not required to provide that person's identity. Nor can the J-Standard's "optional connection test message" satisfy the mandate of section 105. USTA Opp. 4. As its title plainly indicates, this message is "optional." Moreover, even if a carrier 'opts' to provide it, the description of the message in the J-Standard does not ensure that adequate information will be provided to indicate whose facilities an interception is surveilling.

reasonable time upon discovery." SSI Order App. A, § 64.2103(e). We respectfully requested that language be added to this standard to specify the interests that underlie the "reasonability" determination. In support of this request, we explained that unless the relevant interests are specified, carriers can be expected to justify reporting delays by reference to their own business necessity or convenience, and that the Commission and the Department, lacking access to the pertinent information regarding the carrier's internal operations, would be unable to evaluate such claims. Petition 10.

Several commenters assert that our concerns are merely speculative, and assure the Commission that carriers will not delay the reporting of compromises. Yet the commenters themselves disprove this assertion. Indeed, one carrier commenter reserves the right to delay reporting compromises for as long as it takes to "investigat[e] the situation" — a process that may take "hours or days." SBC Opp. 4. Another expressly acknowledges that its "reasonableness" calculation will include a variety of factors unrelated to personal privacy and security, among which will be "technical glitches, human error [and its] own internal investigation." AT&T Opp. 9; see also Bell Atlantic Opp. 5 ("There is no reason to limit the factors that go into a determination of 'reasonableness[]'"); BellSouth Opp. 16 ("The existing rule appropriately allows carriers flexibility when reporting security breaches"); USTA Opp. 5 (arguing that the statute forbids the Commission from "tip[ping] th[e] balance in favor of law enforcement").

These commenters make our case for us. They show that, unless the "reasonableness" standard is modified to require carriers to give precedence to concerns relevant to the language and purposes of section 105, they will in some situations seek to justify substantial delays by reference to an unlimited (Bell Atlantic Opp. 5) reserve of "flexib[le]" (BellSouth Opp. 16) explanations. To

prevent the effective nullification of its regulation, the Commission should add language specifying the interests that must be given precedence in the "reasonability" determination.

4. **Recording Of The Date And Time Of The "Opening Of The Circuit" For Law Enforcement**

Finally, our Petition noted that the SSI Order modified language pertaining to the carriers' recordkeeping obligations proposed in the section 105 Notice of Proposed Rulemaking (SSI NPRM), replacing the proposed obligation to record "the start date and time of [an] interception" (SSI NPRM (rel. Oct. 10, 1997) ¶ 32) with an obligation to record "the start date and time of the *opening of the circuit* for law enforcement." SSI Order ¶ 44; *id.* App. A § 64.2104(a)(1)(ii) (emphasis added). We explained that this language is contrary to the plain language of 47 U.S.C. § 229(b), which requires carriers to maintain records of "any interception," and we requested that the language be modified to require the recording of the "date and time at which the interception of communications or access to call identifying information was enabled." Petition 11.

Only three commenters address this request, and two of them do not appear to disagree with the Department's position. One states that "a carrier is only in a position to record the date and time when a translation is placed in a switch related to the surveillance target." SBC Opp. 4. Assuming, as seems appropriate, that this commenter refers to the process of enabling an interception by effecting the necessary configurations in the switch, this statement is entirely consistent with the Department's request. Another states that "[c]arrier personnel can only record the time a wiretap is

implemented or taken down pursuant to a specific order." CTIA Opp. 8. This, too, appears to be fully consistent with the Department's request.⁴

Only one commenter presents arguments that clearly seek to undermine our requested modification, but its arguments present no sound reason to reject it. The commenter states that carriers already "routinely" maintain the pertinent interception records. AT&T Opp. 9. But that practice could only undermine any claim that the request would impose a burden on carriers, because it shows that the request would merely obligate carriers to include in their surveillance records information they already "routinely" record. The commenter also refers to the fact that some carriers have several different switch platforms installed within their networks. *Id.* at 9-10. This observation is irrelevant. The variety of a carrier's platforms has no effect upon the difficulty of recording the dates and times at which it implements interceptions on any one of them; nor does the recordkeeping mandate of 47 U.S.C. § 229 require any "reconfigur[ation]" of a carrier's switches. *Id.* at 10.

Because the "opening of the circuit" language in the implementing regulations conflicts with the mandate of 47 U.S.C. § 229, the Commission should modify this language to bring the regulation in line with the statute.⁵

⁴This commenter also states that the J-Standard "provides for an electronic message to be sent to law enforcement each time a content channel is opened or closed for a particular interception." CTIA Opp. 7. Of course, the existence of related or similar functions in the J-Standard could not erase the recordkeeping mandate of 47 U.S.C. § 229. At any rate, the statement is misleading, because the J-Standard messages indicate the beginning and end of individual *calls* — not of *interceptions*.

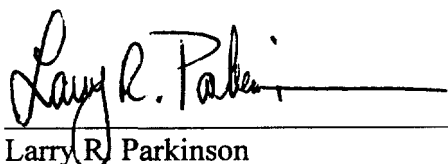
⁵One commenter briefly expresses its support for the National Telephone Cooperative Association's request that the Commission exempt small, rural telephone companies from the mandate to file systems security and integrity policies and procedures with the Commission. PCIA Opp. 6 (citing Petition for Reconsideration and/or Clarification of National Telephone Cooperative Association, October 25, 1999 (NTCA Petition)). As we explained in our February 7, 2000 response and partial
(continued...)

Conclusion

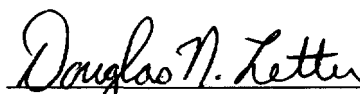
The Department does not lightly ask the Commission to modify its section 105 regulations. All of the modifications requested in our Petition derive from discussions involving federal, state, and local law enforcement agencies, and they represent the matters that the law enforcement community considers most crucial to the achievement of section 105's public purposes. The Department respectfully asks the Commission to consider, and adopt, these modifications.

DATE: February 17, 2000

Respectfully submitted,



Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535



Douglas N. Letter
Appellate Litigation Counsel
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530

⁵(...continued)

opposition to the NTCA Petition, however, the Commission's conclusion that such a distinction would contravene the statute's plain language is unimpeachable, and nothing in this commenter's remarks tends to undermine this conclusion.

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of:)

Communications Assistance for Law)
Enforcement Act)
_____)

CC Docket No. 97-213

Certificate of Service

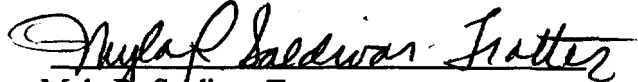
I, Myla R. Saldivar-Trotter, of the Federal Bureau of Investigation, Washington, D.C., hereby certify that, on February 17, 2000, I caused to be filed the original and eleven (11) copies of the foregoing DOJ/FBI Reply to Oppositions to Petition for Reconsideration of Section 105 Report and Order, and served copies of the same by First Class Mail, or by hand where noted, upon the parties identified on the attached service list.

DATED at Washington, D.C. this 17th day of February, 2000.


Myla R. Saldivar-Trotter

Certificate of Service

I, Myla R. Saldivar-Trotter, Federal Bureau of Investigation, hereby certify that a true copy of the foregoing DOJ/FBI Reply to Oppositions to Petition for Reconsideration of Section 105 Report and Order was served via hand delivery (indicated by *) or by mail to the following parties:


Myla R. Saldivar-Trotter

The Honorable William E. Kennard*
Chairman
Federal Communications Commission
445 Twelfth Street, S.W., Room 8B201
Washington, D.C. 20554

Ari Fitzgerald*
Legal Advisor to Chairman Kennard
Federal Communications Commission
445 Twelfth Street, S.W., Room 8B201
Washington, D.C. 20554

The Honorable Harold Furchtgott-Roth*
Commissioner
Federal Communications Commission
445 Twelfth Street, S.W., Room 8A302
Washington, D.C. 20554

The Honorable Susan Ness*
Commissioner
Federal Communications Commission
445 Twelfth Street, S.W., Room 8B115
Washington, D.C. 20554

The Honorable Michael Powell*
Commissioner
Federal Communications Commission
445 Twelfth Street, S.W., Room 8A204
Washington, D.C. 20554

The Honorable Gloria Tristani*
Commissioner
Federal Communications Commission
445 Twelfth Street, S.W., Room 8C302
Washington, D.C. 20554

Mark Schneider*
Legal Advisor To Commissioner Ness
Federal Communications Commission
445 Twelfth Street, S.W., Room 8B115B
Washington, D.C. 20554

Bryan Tramont*
Legal Advisor to
Commissioner Furchtgott-Roth
Federal Communication Commission
445 Twelfth Street, S.W., Room 8A302B
Washington, D.C. 20554

Peter Tenhula*
Legal Advisor to Commissioner Powell
Federal Communications Commission
445 Twelfth Street, S.W., Room 8A204F
Washington, D.C. 20554

Karen Gulick*
Legal Advisor To Commissioner Tristani
Federal Communications Commission
445 Twelfth Street, S.W., Room 8C302F
Washington, D.C. 20554

Christopher J. Wright*
General Counsel
Federal Communications Commission
445 Twelfth Street, S.W., Room 8C755
Washington, D.C. 20554

Thomas Sugrue*
Bureau Chief
Wireless Telecommunications Bureau
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Kent Nilsson *
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Jim Burtle*
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Rodney Small*
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, S.W., Room 7A121
Washington, D.C. 20554

Charlene Lagerwerff*
Wireless Telecommunications Bureau
Federal Communications Commission
445 Twelfth Street, S.W., Room 4A124
Washington, D.C. 20554

Tejal Mehta*
Wireless Telecommunications Bureau
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Lawrence E. Strickling*
Chief
Common Carrier Bureau
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Anna Gomez*
Chief
Network Services Division
Common Carrier Bureau
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Charles Iseman*
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Julius Knapp*
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Geraldine Matisse*
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

James F. Green*
Wireless Telecommunications Bureau
Federal Communications Commission
445 Twelfth Street, S.W., Room 4A237
Washington, D.C. 20554

David O. Ward*
Network Services Division
Common Carrier Bureau
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Dale Hatfield *
Chief
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Diane Conley*
Wireless Telecommunications Bureau
Federal Communications Commission
445 Twelfth Street, S.W., 4th Floor
Washington, D.C. 20554

Matthew J. Flanigan, President
Grant Seiffert, Vice President
Government Relations
Telecommunications Industry Association
Suite 300, 2500 Wilson Boulevard
Arlington, VA 22201-3834

Thomas Wheeler
President & CEO
Cellular Telecommunications Industry
Association
Suite 200, 1250 Connecticut Avenue, N.W.
Washington, D.C. 20036

Mark J. Golden
Senior Vice President, Industry Affairs
Robert Hoggarth
Senior Vice President, Paging/Messaging
Personal Communications Industry Association
Suite 700
500 Montgomery Street
Alexandria, VA 22314-1561

Alliance for Telecommunication Industry
Solutions
Suite 500
1200 G. Street, N.W.
Washington, D.C. 20005

Susan Aaron*
Office of General Counsel
Federal Communications Commission
445 Twelfth Street, S.W., Room 8A522
Washington, D.C. 20554

David Krech*
Wireless Telecommunications Bureau
Federal Communications Commission
445 Twelfth Street, S.W., Room 4A223
Washington, D.C. 20554

Stewart A. Baker
Tom Barba
Steptoe & Johnson, LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036-1795

Albert Gidari
Perkins Coie
1201 Third Avenue
40th Floor
Seattle, Washington 98101

Roy Neel
President & CEO
United States Telephone Association
Suite 600
1401 H Street, N.W.
Washington, D.C. 20005-2164

Jerry Berman
Executive Director
Center for Democracy and Technology
Suite 1100
1634 Eye Street, N.W.
Washington, D.C. 20006

Mark C. Rosenblum
Ava B. Kleinman
Seth S. Gross
Room 3252F3
295 North Maple Avenue
Basking Ridge, NJ 07920

Pamela J. Riley
David A. Gross
AirTouch Communications, Inc.
1818 N Street, N.W.
Washington, D.C. 20036

James P. Lucier, Jr.
Director of Economic Research
Americans for Tax Reform
Suite 200
1320 Eighteenth Street, N.W.
Washington, D.C. 20036

Anita Sheth
Director, Regulatory Policy Studies
Citizens for a Sound Economy
Suite 700
1250 H Street, N.W.
Washington, D.C. 20005

Eric W. DeSilva
Stephen J. Rosen
Wiley, Rein & Fielding
1776 K Street, N.W.
Washington, D.C. 20006

Michael Altschul
Vice President and General Counsel
Randall S. Coleman
Vice President, Regulatory Policy and Law
Cellular Telecommunications Industry Association
Suite 800, 1250 Connecticut Avenue, N.W.
Washington, D.C. 20036

William L. Roughton, Jr.
Associate General Counsel
PrimeCo Personal Communications, L.P.
Suite 320 South
601 Thirteenth Street, N.W.
Washington, D.C. 20005

Joseph R. Assenzo
4900 Main Street, 12th Floor
Kansas City, MO 64112

Lisa S. Dean
Director, Center for Technology Policy
Free Congress Foundation
717 Second Street, N.E.
Washington, D.C. 20002

James X. Dempsey
Senior Staff Counsel
Daniel J. Weitzner
Deputy Director
Center for Democracy and Technology
Suite 1100
1634 Eye Street, N.W.
Washington, D.C. 20006

Lawrence E. Sarjeant
Linda Kent
Keith Townsend
John W. Hunter
Julie E. Rones
United States Telecom Association
Suite 600, 1401 H Street, N.W.
Washington, D.C. 20005

John Pignataro
Senior Technical Advisor
Police Department, City of New York
Fort Totten Building 610
Bayside, NY 11359

Barbara J. Kern
Counsel
Ameritech Corporation
4H74
2000 Ameritech Center Drive
Hoffman Estates, IL 60196

Robert Vitanza
Senior Counsel
Cellular One
480 East Swedesford Road
Wayne, PA 19087

S. Kendall Butterworth
BellSouth Cellular Corp.
Suite 910
1100 Peachtree Street, N.E.
Atlanta, GA 30309-4599

J. Lloyd Nault, II
BellSouth Telecommunications, Inc.
4300 BellSouth Center
675 West Peachtree Street, N.E.
Atlanta, GA 30375

Kurt A. Wimmer
Gerard J. Waldron
Alane C. Weixel
Ellen P. Goodman
Erin Egan
Covington & Burling
1201 Pennsylvania Avenue, N.W.
P.O. Box 7566
Washington, D.C. 20044-7566

Kathryn Marie Krause
Edward M. Chavez
1020 Nineteenth Street, N.W.
Washington, D.C. 20036

James D. Ellis
Robert M. Lynch
Durward D. Dupre
Lucille M. Mates
Frank C. Magill
175 E. Houston, Room 4-H-40
San Antonio, TX 78205

M. Robert Sutherland
Angela N. Brown
BellSouth Corporation
Suite 1700
1155 Peachtree Street, N.E.
Atlanta, GA 30309-3610

Michael W. White
BellSouth Wireless Data, L.P.
10 Woodbridge Center Drive, 4th Floor
Woodbridge, NJ 07095-1106

Charles M. Nalbourne
Suite 400
3353 Peachtree Road, N.E.
Atlanta, GA 30326

William T. Lake
John H. Harwood, II
Samir Jain
Todd Zubler
Wilmer, Cutler & Pickering
2445 M Street, N.W.
Washington, D.C. 20037-1420

John M. Goodman
Attorney for Bell Atlantic
1300 I Street, N.W.
Washington, D.C. 20005

Martin L. Stern
Lisa A. Leventhal
Preston Gates Ellis & Rouvelas Meeds LLP
Suite 500
1735 New York Avenue, N.W.
Washington, D.C. 20006

Cheryl A. Tritt
James A. Casey
Morrison & Foerster LLP
Suite 5500
2000 Pennsylvania Avenue, N.W.
Washington, D.C. 20006

Sylvia Lesse
Marci Greenstein
Kraskin, Lesse & Cosson, LLP
2120 L Street, N.W.
Suite 520
Washington, D.C. 20037

Henry M. Rivera
Larry S. Solomon
J. Thomas Nolan
Shook, Hardy & Bacon LLP
Suite 900
1850 K Street, N.W.
Washington, D.C. 20006

John T. Scott, III
Crowell & Moring LLP
1001 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Carole C. Harris
Christine M. Gill
Anne L. Fruehauf
McDermott, Will & Emery
600 Thirteenth Street, N.W.
Washington, D.C. 20005

Francis D. R. Coleman
Director of Regulatory Affairs
- North America
ICO Global Communications
Suite 550
1101 Connecticut Avenue, N.W.
Washington, D.C. 20036

Joel M. Margolis
Corporate Counsel-Regulatory
Nextel Communications, Inc.
Suite 100
1505 Farm Credit Drive
McLean, VA 22102

Alfred G. Richter, Jr.
Roger K. Toppins
Hope E. Thurrott
SBC Communications, Inc.
One Bell Plaza, Room 3023
Dallas, TX 75202

Colette M. Capretz
Fisher Wayland Cooper
Leader & Zaragoza LLP
Suite 400
2001 Pennsylvania Avenue, N.W.
Washington, D.C. 20006

Lon C. Levin
Vice President and Regulatory Counsel
American Mobile Satellite Corporation
10802 Park Ridge Boulevard
Reston, VA 20191

Edward J. Wisniewski
Deputy Assistant Administrator
Office of Investigative Technology
Drug Enforcement Administration
8198 Terminal Road
Lorton, VA 22079

Peter M. Connolly
Koteen & Naftalin, LLP
1150 Connecticut Avenue, N.W.
Washington, D.C. 20036

L. Marie Guillory
Jill Canfield
National Telephone Cooperative Association
4121 Wilson Boulevard, 10th Floor
Arlington, VA 22203-1801

Stephen C. Garavito
Martha Lewis Marcus
Room 1131M1
295 North Maple Avenue
Basking Ridge, NJ 07920

Mary McDemott, Sr. Vice President/Chief of Staff
Government Relations
Robert L. Hoggarth, Sr. Vice President
Paging and Narrowband
Todd B. Lantor, Director
Government Relations
Personal Communications Industry Association
Suite 700, 500 Montgomery Street
Alexandria, VA 22314

Stewart A. Baker
Thomas M. Barba
L. Benjamin Ederington
Matthew L. Stennes
Steptoe & Johnson, LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036

Colonel Carl A. Williams
Superintendent, New Jersey State Police
P.O. Box 7068
West Trenton, NJ 08628-0068

Dudley M. Thomas
Director, Texas Department of Public Safety
5805 N. Lamar Boulevard
Box 4087
Austin, TX 78773-0001

Roseanna DeMaria
AT &T Wireless
Room 1731
32 Avenue of the Americas
New York, NY 10013

Anne F. La Lena
MCI WorldCom, Inc.
1801 Pennsylvania Avenue, N.W.
Washington, D.C. 20006

Rich Barth
Vice President and Director,
Telecommunications Strategy
Mary Brooner
Director, Telecommunications Strategy
Motorola, Inc.
Suite 400, 1350 I Street, N.W.
Washington, D.C. 20005